U.S. Department of Transportation
United States Coast Guard

Commandant G-TTO

MAILING ADDRESS:

U. S. COAST GUARD
2100 SECOND STREET S.W.
WASHINGTON, DC 20593-0001
(202) 267-0730

COMDTINST 2023.1

17 APR 1992

COMMANDANT INSTRUCTION 2023.1

Subj: High Frequency Data Link (HFDL) Shipboard System Security Procedures

Ref: (a) COMDTINST M5500.13A (Automated Information Systems Security Manual)
(b) COMDTINST M5500.17 (Standard Workstation Security Handbook)
(c) COMDTINST M5500.11A (Security Manual)
(d) CSP-1 (Cryptographic Security and COMSEC Material Policies)
(e) CMS4 (Communications Security Material System CMS Manual)
(f) COMDTINST 5520.9 (Centralization of U.S. Coast Guard Military Security Clearance and Eligibility)
(g) COMDTINST M5510.16 (Military Personnel Security Program)

1. PURPOSE. The purpose of this Instruction is to provide specific procedures for shipboard security of the High Frequency Data Link (HFDL) system which is part of each unit's Secure Electrical Information Processing System (SEIPS). This Instruction is for use by all Coast Guard afloat units with HFDL installed.

2. DIRECTIVE AFFECTED. None

DISTRIBUTION - SDL No. 130

| | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | | | | | 1 | | | | 1 | | | | 1 | 1 | | | | | | | | 1 | | | | |
| B | | 8 | 20 | | | | | | | | | | 1 | | | | | 1 | | | | | | | | |
| C | | | | | | | | | | | | | | | | | 1 | | | | | | | | | |
| D | | | | | | | | | | | | | | | | | | | | | | | | | | |
| E | | | | | | | | | | | | | | | | | | | | | | | | | | |
| F | | | | | | | | | | | | | | | | | | | | | | | | | | |
| G | | | | | | | | | | | | | | | | | | | | | | | | | | |
| H | | | | | | | | | | | | | | | | | | | | | | | | | | |

• NON-STANDARD DISTRIBUTION:

3. BACKGROUND. The HFDL system is the first Automated Information System (AIS) installed on vessels smaller than Medium Endurance Cutters and authorized to transfer and store classified information. As these systems are fielded, careful attention to management of security risks is required. Increasing reliance on AISs to accomplish much of our work demands that we recognize and manage risks associated with using such systems. References listed above outline specific procedures for administering and managing these systems. Due to the large number of instructions and manuals, this Instruction is provided as a more convenient guide to assist in navigating the security and accreditation process for new installations.

4. HFDL VESSEL REQUIREMENTS. Commanding officers of units receiving HFDL installations shall ensure the following are accomplished:

   a. Request a Visual TEMPEST Configuration Control Inspection (VTCCI) immediately after installation is completed. Units that have not already requested this inspection should do so immediately. Requests for VTCCI should be in the form of a message to the appropriate MLC and District office (sample message in enclosure (2)).

   b. Designate an Automatic Data Processing Systems Security Officer (ADPSSO) in writing as per reference (a). (This designation can be combined with other job designations.)

   c. Provide input to the area and district office AIS Security Plans as per reference (a) chapter 13 (sample in enclosure (2)). Review enclosure (1) and make revisions as necessary for your unit, then add this unit AIS security plan to the HFDL System Documentation three-ring binder.

   d. Ensure that passwords are applied to the system as per reference (b).

   e. Label all removable hard disks and floppy disks with appropriate classification labels. Classified media shall be entered into the unit's Classified Material Control System Log as per reference (c).

4. f. Assist the area's and district (dt's) in preparing a risk assessment as per reference (a) chapter 13.

   g. Prepare a contingency plan as per reference (a) (enclosure (3) is provided as a sample unit plan).

   h. Dispose of laser printer toner cartridges, that have exhausted their toner, as unclassified waste after running one additional unclassified page through the printer.

   i. Update the unit's Emergency Action Plan (EAP) to include procedures for disposition or destruction of the System KEYMAT, hard disk(s), and any other associated classified backup tapes or floppy disks in accordance with reference (d) and (e).

5. AUTHORIZED HFDL EQUIPMENT CONFIGURATIONS. The security controls identified in this instruction meet minimum requirements for AIS security. All HFDL SEIPS installed to date and operated as per this Instruction are hereby granted interim authority to operate. This interim authority will expire one year from the date of this Instruction. Units must comply with the requirements in paragraph 4 (a-e) and be actively pursuing compliance with paragraph 4 (f-i). This Instruction is provided, in part, to assist in preparing the documentation required.

   a. **HFDL SEIPS is a stand alone terminal and SHALL NOT be clustered to any other workstations.**

   b. Since a 25-pin TEMPEST approved A/B switch is not currently available, units are not authorized to share the HFDL laser printer with the administrative terminal using an A/B switch.

   c. No other configuration modifications are permitted without the express permission of Commandant (G-TPS-4).

6. PHYSICAL SECURITY UNDERWAY. Each HFDL system is a Secure Electrical Information Processing System (SEIPS).

   a. Access to HFDL systems is limited to those personnel with need to know, holding proper access and clearance. Units unable to provide a separate secure space for the SEIPS (110's, SES's, 140's) must ensure all unit personnel maintain a clearance equal to that of the KEYMAT loaded. Reference (f) describes the Coast Guard security clearance procedures that delegate Commanding Officer's authority to grant interim SECRET clearances. Final SECRET clearances are now granted by the Department of Navy Central Adjudication Facility (DONCAF). Commanding Officers should use OPNAV 5510 to request a final SECRET from DONCAF (coordinate with your local PERSRU for further assistance).

   b. Visitors are not permitted access to an area containing an operational HFDL system without a cleared escort. The escort must ensure the system and surrounding area are sanitized prior to allowing access to visitors. Visual barriers, such as shower curtains, are not required.

   c. Storage of the HFDL system Key Material (KEYMAT) must comply with the Two Person Integrity (TPI) procedures outlined in references (d) and (e). Personnel handling KEYMAT must also adhere to these procedures. Viewing the KEYMAT loading evolution is strictly limited to those with the need to know and who have properly documented access and clearance.

7. PHYSICAL SECURITY IN-PORT.

   a. Units unable to provide a secure space for HFDL SEIPS: In-port operation of the HFDL system must be constantly attended and visitor access limited as described in paragraph (6.b.) of this Instruction. Before unmanning the HFDL space, the classified removable hard disk shall be stored in a GSA approved security container, the KG-84C shall be zeroized, and the printer shall be turned off. **Vessels with HFDL fixed disk systems shall ensure both locking bars are secured in place to restrict access to the tape drive, floppy drive, and keyboard port.**

7. b. Units with secure HFDL spaces:
Unattended in-port operation of the HFDL system may be conducted when installed in a restricted area as defined in reference (c).

c. All HFDL vessels:
The Coast Guard Standard Workstation (CGSW) used for HFDL and equipped with removable hard disks may be used for administrative purposes provided the steps outlined in enclosure (1) are followed exactly. **This does not apply to units with fixed disk systems. Fixed disk HFDL systems SHALL NOT be operated as administrative terminals.** The remaining fixed hard disk HFDL systems should be replaced with removable hard disks in the near future.

8. ACTION. Area and district commanders, their security managers, their Automated Data Processing Security Officers (ADPSOs), Commanders of Maintenance and Logistics Commands, and unit commanding officers, shall ensure the procedures and policies stated herein are followed.

W. J. PCLANT
Chief, Office of Command, Control & Communications

Encl: (1) Sample HFDL AIS Security Plan
(2) Sample HFDL Request for VTCCI, and required input to District AIS Security Plan
(3) Sample HFDL Contingency Plan

Enclosure (1) to COMDTINST 2023.1

**USCGC AFLOAT HIGH FREQUENCY DATA LINK (HFDL)**

**AUTOMATED INFORMATION SYSTEM (AIS) SECURITY PLAN FOR**

**USCGC _____**

References:

(a) COMDTINST M5500.11A (Security Manual)

(b) COMDTINST M5500.13A (Automated Information Systems Security Manual)

(c) COMDTINST 5520.9 (Centralization of U.S. Coast Guard Military Security Clearance and Eligibility)

(d) COMDTINST M5510.16 (Military Personnel Security Program)

(e) CMS4 (Communications Security Material System CMS Manual)

(f) CSP-1 (Cryptographic Security and COMSEC Material Policies)

(g) COMDTINST M5500.17 (Standard Workstation Security Handbook)

I. BACKGROUND:

The following Security Plan is provided for a quick overview of specific procedures relating to the Coast Guard High Frequency Data Link (HFDL) System. These do not take the place of the above references which all HFDL operators should become familiar with prior to becoming qualified as an HFDL operator. The HFDL System Software and Documentation three-ring binder describes specific procedures for system operation. Add the HFDL AIS Security Plan to the front of the HFDL System Software and Documentation three-ring binder provided with your system installation, so it is available for future reference.

II. GENERAL:

The HFDL system uses the vessel's standard High Frequency (HF) radio equipment suite to send/receive error free record message traffic up to and including SECRET when equipped with the appropriate Keying Material (KEYMAT). The system was designed for vessels operating without RMs assigned, to provide hands-off message delivery. The HFDL system installed is a stand alone Coast Guard Standard Workstation (CGSW) and includes the following equipment:

II. a. CGSW - 386 or 286 Central Processing Unit (CPU)
Floppy Drive Module
(2) 44MB Removable Hard Disk Modules. (Vessels using fixed disks change this to read 69MB Hard Disk)
Canon LBP4 or LBP8 Mark III Laser Printer

b. Encryption Device - KG-84C

c. HF Modem - Harris 3466A Universal Modem

d. UPS - Clary uninterruptable power supply

III. AUTHORIZED HFDL EQUIPMENT CONFIGURATIONS:

The HFDL system is only authorized for use in the configuration installed. No system configuration changes are authorized or permitted without prior approval of Commandant (G-TPS-4) and notification to your Designated Approving Authority (DAA). **Because of security considerations the HFDL Secure Electrical Information Processing System (SEIPS) shall not be clustered to any other workstations.**

Use of an A/B switch to share the Laser printer with the administrative terminal is not authorized.

IV. PHYSICAL SECURITY UNDERWAY:

The HFDL system is a Secure Electrical Information Processing System (SEIPS) as defined in MIL-STD-1680B. Access to the HFDL SEIPS is limited to personnel with a need to know and who hold proper access and clearance.

a. Visitors are not permitted access the area containing the HFDL system when operating without a cleared escort. The escort must ensure the system and area surrounding are sanitized prior to allowing access to visitors. To sanitize the HFDL system, secure all classified information in the area, and blank the system's video screen. The screen can be blanked manually by turning down the system video brightness control.

b. Storage of the HFDL system Key Material (KEYMAT) shall comply with the Two Person Integrity (TPI) procedures outlined in references (e) and (f). System operators shall maintain TPI while participating in loading and destroying KEYMAT evolutions. Viewing of these evolutions is limited to personnel having a need to know and holding the required documented access and clearance.

IV. c. All removable hard disks and floppy disks shall have the appropriate classification labels on them. Classified media must be entered into the unit's Classified Material Control System log in accordance with COMDTINST M5500.11A (Security Manual). The classified HFDL system hard disk(s) must have a classification label corresponding to the classification of the KEYMAT loaded.

V. PHYSICAL SECURITY IN-PORT:

a. Vessels unable to provide a secure space for HFDL SEIPS: In port operation of the HFDL system shall be constantly attended and visitor access limited as described in para (IV.a.). Before unmanning this HFDL space, the classified removable hard disk shall be removed from the workstation, stored in a GSA approved security container, the KG-84C shall be ZEROIZED, and the laser printer shall be powered off. **Vessels with HFDL fixed disk systems must ensure both locking bars are in place to restrict access to the tape drive, floppy drive, and keyboard port.**

b. Vessels with secure HFDL spaces: Unattended in-port operation of the HFDL system may be conducted when installed in a restricted area as defined in reference (a).

VI. CONVERTING HFDL SEIPS WITH REMOVABLE HARD DISK TO USE AS AN ADMINISTRATIVE TERMINAL:

The Coast Guard Standard Workstation (CGSW) used for HFDL, and equipped with removable hard disks, may be used for administrative purposes provided the steps outlined below are followed exactly. Ensure that all HFDL users are made aware of these minimum procedures prior to being allowed to convert the HFDL terminal to administrative purposes and use by administrative personnel. **These guidelines do not apply for fixed disk HFDL systems. Fixed disk HFDL SEIPS shall not be used as an administrative terminal.**

a. Remove the Classified HFDL Hard Disk from the drive module and store in a GSA approved security container.

b. Zeroize the KG-84C and power off at the front panel switch.

c. Power off the Harris modem with the front panel switch.

d. Power off the HFDL CGSW CPU module to clear Random Access Memory (RAM).

e. Power off the HFDL printer to clear any queued messages.

VI. f. Insert an unclassified hard disk containing the necessary files for operating as an administrative terminal.

g. Power on the CGSW CPU module.

VII. LASER PRINTER TONER CARTRIDGE DISPOSAL:

When HFDL laser printer toner cartridges have exhausted their toner, the cartridges may be disposed of as unclassified waste after running one additional unclassified page through the printer. For the Canon LBP4 or LBP8 Mark III, ensure the "On Line" button is lit, then press the front panel "On Line" button, (light goes out) followed by the "Test/Font" button. This will cause the printer to generate one test page of data and will ensure no sensitive print is available on the cartridge.

**SAMPLE VTCCI REQUEST MESSAGE**

P XXXXXXZ
FM USCGC **NEWHFDL**
TO COMCOGARD MLC(**PAC or LANT**)//TTS-3//
CCGD(**Applicable District for District units**)//DT//
COMXXXXAREA COGARD (**Applicable Area for Area units**)//AT or PT//
INFO COMDT COGARD WASHINGTON DC//G-TTO-2/G-TTO-3/G-TPS-4//
COGARD ISC ALEXANDRIA VA//ISCTT1//
ACCT W2-**XXXX**
BT
UNCLAS //N02023//
SUBJ: INSTALLATION OF HFDL SYSTEM ABOARD USCGC **NEWHFDL**
MSGID/GENADMIN/USCGC **NEWHFDL**//
REF/A/DOC/COMDTINST//
AMPN/2023.1, SUBJECT: HFDL SHIPBOARD SYSTEM SECURITY PROCEDURES//
REF/B/DOC/COMDTINST/24JUL87//
AMPN/M5500.13A, SUBJECT: AIS SECURITY MANUAL, PG 13-4//
RMKS/
1. INSTALLATION OF THE SUBJECT SYSTEM WAS COMPLETED ABOARD USCGC **NEWHFDL** BY (**INSTALLER**) ON (**DATE**).
2. ORIGINATOR HAS BEEN PROVIDED WITH THE REQUIRED OPERATING MANUALS AND TWO BACK UP SYSTEM REMOVABLE HARD DISKS.
3. ORIGINATOR HAS IMPLEMENTED THE SECURITY POLICY IDENTIFIED IN REF A AND IS ACTIVELY WORKING ON COMPLETION OF THE REQUIRED CONTINGENCY PLANNING DOCUMENT.
4. SYSTEM TRAINING WAS PROVIDED BY (**NAME**) FOR (**NUMBER**) ASSIGNED PERSONNEL.
5. REQUEST DISTRICT (Area for area units) ADD THIS HFDL SEIPS TO THEIR AIS SECURITY PLAN.
6. REQUEST DISTRICT ASSISTANCE IN PREPARING THE RISK ASSESSMENT IAW REF B. POC: (**QM1 I.M. HFDL**) (**PHONE**)
7. FOR MLC: REQUEST VTCCI BE SCHEDULED AT EARLIEST POSSIBLE DATE.//
BT

**USCGC _____ HFDL CONTINGENCY AND DISASTER PLANNING**

References:

(a) COMDTINST 2023.1 (HFDL AIS Security Plan)

(b) HFDL Acquisition and Support Plan (In approval process)

(c) HFDL System Software and Documentation (3 ring binder)

(d) USCGC _____ Emergency Action Plan

(e) COMDTINST M5500.13A (AIS Security Manual)

**PURPOSE:** This contingency plan provides a course of action to be taken during or following an emergency or other abnormal event which causes or may cause a disruption in data processing services for the High Frequency Data Link system.

**CONTROLS:** These are the physical, personnel, administrative, hardware, software, or communications measures used to protect against unauthorized (accidental or intentional) disclosure, modification, or destruction of the HFDL system or system data.

a. Physical and personnel control of the HFDL Secure Electrical Information Processing System (SEIPS) shall comply with reference (a).

b. Administrative controls consist of ensuring there is ***ALWAYS A BACK-UP SYSTEM HARD DISK AVAILABLE*** in case of disk media failure. The system manager shall apply the same protection practices to the back-up removable hard disk that are applied to the active system removable hard disk. A third back-up hard disk is highly recommended for storage at an alternate site, but not required. **Fixed disk HFDL systems must maintain at least one back-up QIC tape. A third back-up is highly recommended for storage at an alternate site, but not required.**

c. The HFDL System Software and Documentation three-ring binder contains system documentation, trouble shooting procedures, and extra removable hard disks. Ensure this documentation is easily accessible in the HFDL operation area.

d. Operational back up to the HFDL record message system is provided by the secure voice suite (ANDVT/VINSON). HFDL equipment failure while in an operational posture should be reported to the District OPCON as soon as possible to initiate casualty recovery. Initiate a CASREP message in accordance with the appropriate MLC SOP and COMDTINST M3501.3(Series). Maintenance and replacement duties and procedures are discussed in the Acquisition and Support Plan (ASP). Refer to this document for any equipment outages.

**EMERGENCY RESPONSES:** The objective of emergency response is to prevent or minimize injury/damage to personnel and/or to the HFDL system.

a. FIRE:

1. Objective: Protect lives and ensure safety of facility personnel. **Under no circumstances shall anyone subject themselves or their subordinates to death or injury to protect these materials from fire.** Minimize damage to data and facility resources associated with the HFDL system.

2. Actions:
   (a) Turn off all power to all HFDL equipment at the circuit breaker located _____ and labeled _____.
   (b) If fire is localized, visible, and the fire alarm has not sounded, attempt to extinguish using hand held fire extinguishers located _____.
   (c) If the fire cannot be put out immediately, activate the fire alarm by __(HOW)_____ and evacuate the area, closing all doors when leaving.
   (d) Notify the Officer of the Deck (OOD) by the fastest means possible when underway. If in port, notify the OOD, and follow the appropriate ship's procedure for fire in port.

b. WATER DAMAGE:

1. Objective: Minimize damage to data, electronic equipment and other facility resources.

2. Actions:
   (a) Turn off all power to all HFDL equipment at the circuit breaker located _____ and labeled _____.

b. 2. (b) If water source is overhead, cover equipment with water repellent tarpaulins or plastic covers.
(c) Move material (e.g. floppies, supplies) that may be affected by water to elevated positions or to alternate storage locations.
(d) Notify the OOD and Automated Data Processing Systems Security Oficer (ADPSSO).

c. POWER FAILURE:

1. Objective: Minimize damage to electronic components and data stored on fixed media.

2. Actions:
(a) Turn off all power to all HFDL equipment at the circuit breaker located _____ and labeled _____.
(b) Notify OOD and ADPSSO.
(c) Shut off individual power switches to each HFDL module and ensure all individual power switches remain in OFF position until power is returned and determined by OOD to be stable.

d. COMMUNICATIONS FAILURE:

1. Objective: Minimize duration and effects of loss of communications links.

2. Actions:
(a) Notify the OOD, Electrical Maintenance Officer (EMO), and ADPSSO.
(b) Attempt to isolate the trouble to one or more specific equipments.
(c) Attempt to establish communications through other means (e.g. ANDVT/VINSON).
(d) Notify district OPCON of system failure using normal unit procedures.

e. SYSTEM HARDWARE FAILURE:

1. Objective: Minimize system downtime; prevent damage to electronic components, applications/system software.

2. Actions:
(a) Notify the OOD and ADPSSO.
(b) HFDL SEIPS is equipped with a back-up removable hard drive module. If you suspect a Hard Drive failure, follow the instructions in the HFDL documentation three-ring binder for operating

e. 2. (b) from the second drive. System operators should refer to this documentation for any other system trouble.
(c) If unsuccessful in returning the system to operation, notify district OPCON using normal unit procedures.

f. SOFTWARE FAILURE:

1. Objective: Minimize damage/loss of data and system availability.

2. Actions:
(a) Document any error messages visible on the screen.
(b) Attempt to reset the system using the warm boot reset button in back of the CPU module.
(c) Notify the ADPSSO if failure persists.
(d) Shut down all power to each component of the system, then power up in the order defined in the HFDL system documentation three-ring binder.
(e) If unsuccessful, remove the system hard disk and attempt to start system with the archive back-up hard disk. **Fixed disk HFDL units should attempt recovery with the back-up QIC tape cartridge.**

g. ILLEGAL/UNAUTHORIZED ENTRY TO FACILITY:

1. Objective: Protect AIS hardware and software. Minimize the risk of damage/loss of data, hardware, and software.

2. Actions:
(a) Request identification. Avoid clash with unauthorized entrant.
(b) Ask entrant to leave ADP premises - note description.
(c) Call ADPSSO, OOD, and Command Security Officer (CSO).
(d) Move vital system documentation to a safer location if necessary.
(e) Assess the likelihood of compromise.

h. THEFT:

1. Objective: To expedite the recovery or replacement of the missing resource(s).

2. Actions:
   (a) Itemize the missing resources.
   (b) Notify the OOD, ADPSSO, and CSO.
   (c) Do not touch anything until proper authorities have arrived.
   (d) Make assessment of the impact on HFDL systems.